CLAIMS

We claim:

1. A method for a service provider to transmit decryption information in a secure manner, comprising:

receiving a request for a service from a requestor over a bi-directional channel;

authenticating the requestor;

transmitting first decryption information to the requestor over the bi-directional channel for use in decrypting the service;

transmitting the service, encrypted with encryption information corresponding to the first decryption information, over a unidirectional channel;

generating second decryption information for use in decrypting the service;

transmitting the second decryption information over the unidirectional channel; and

transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel.

2. The method of claim 1 wherein the first decryption information corresponds to a seed of a macro period and the second decryption information corresponds to a micro period of the macro period.

3. The method of claim 2 wherein the micro period is a first micro period of the macro period.

4. The method of claim 1 wherein the second decryption information is transmitted as future decryption information.

5. The method of claim 1 wherein the first decryption information and the second decryption information correspond to different micro periods of a macro period.

6. The method of claim 1 further comprising:

transmitting future decryption information over the bi-directional channel; and

transmitting the service encrypted with encryption information corresponding to the future decryption information.

7. The method of claim 1 wherein the request for a service is a request for the service in its entirety or a time interval thereof.

8. The method of claim 1 wherein the bidirectional channel is one of a wireless network.

9. The method of claim 8 wherein the wireless network is a GSM network.

10. The method of claim 8 wherein the wireless network is a Bluetooth network.

11. The method of claim 1 wherein the unidirectional channel is one of a DVB-T network.

12. The method of claim 1 wherein the authenticating is performed using a SIM card number.

13. The method of claim 1 wherein the authenticating is performed using a user ID and password.

14. The method of claim 1 wherein the authenticating is performed using IP authentication.

15. The method of claim 14 wherein the IP authentication is a public key encryption scheme.

16. The method of claim 1 wherein the first decryption information is transmitted to the requestor over the bidirectional channel before the service has begun.

17. The method of claim 1 wherein generating second decryption information involves changing a decryption key, a decryption parameter and/or a decryption algorithm of the first decryption information.

18. The method of claim 1 further comprising:

transmitting synchronization information for use by the requestor in determining when the second decryption information is valid.

19. The method of claim 1 further comprising:

encrypting the second decryption information with encryption information corresponding to the first decryption information.

20. The method of claim 1 further comprising:

re-transmitting the second decryption information over the unidirectional channel.

21. A method for a service provider to transmit decryption information in a secure manner, comprising:

receiving a request for a service from a requestor over a bi-directional channel;

authenticating the requestor;

providing decryption information to the requestor over the bi-directional channel for use in decrypting the service;

transmitting the service, encrypted with encryption information corresponding to the decryption information, over a unidirectional channel;

changing the decryption information needed to decrypt the service throughout the transmission of the service; and

providing the requestor with changes to the decryption information over the unidirectional channel.

22. The method of claim 21 wherein the changes to the decryption information are encrypted using encryption information corresponding to decryption information that was previously provided to the requestor.

23. The method of claim 22 wherein the previously provided decryption information was provided over the bidirectional channel.

24. The method of claim 22 wherein the previously provided decryption information was provided over the unidirectional channel.

25. A method for a client to receive decryption information from a service provider in a secure manner, comprising:

requesting a service over a bi-directional channel;

transmitting authentication information over the bi-directional channel;

receiving first decryption information over the bi-directional channel;

receiving the service over a unidirectional channel;

decrypting the service using the first decryption information;

receiving second decryption information over the unidirectional channel; and

decrypting the service using the second decryption information.

26. The method of claim 25, further comprising:

upon completion of the service, requesting another service via the bi-directional channel.

27. The method of claim 25, further comprising:

decrypting the service with the first decryption information until unsuccessful and thereafter decrypting the service with the second decryption information.

28. The method of claim 25 wherein the authentication includes a SIM card number.

29. The method of claim 25 wherein the authentication includes a user ID and password.

30. The method of claim 25 wherein the authentication includes IP authentication.

31. The method of claim 30 wherein the IP authentication is a public key encryption scheme.

32. The method of claim 25 wherein the service is requested during a predetermined window of time.

33. The method of claim 25, further comprising:

determining whether the service has been dropped;

if the service has been dropped,

determining whether either the first decryption information or the second decryption information is valid decryption information;

if one of the first decryption information or the second decryption information is valid decryption information,

decrypting the service with the valid decryption information.

34. The method of claim 33, further comprising:

if nether the first decryption information nor the second decryption information is valid decryption information,

establishing a connection to the service provider via the bi-directional channel;

transmitting authentication information over the bi-directional channel;

receiving valid decryption information over the bi-directional channel; and

decrypting the service using the valid decryption information.

35. The method of claim 25, further comprising:

receiving synchronization information for determining when the second decryption information is valid.

36. The method of claim 25, further comprising:

receiving and storing one or more future keys for decrypting the service after the first and second decryption information are no longer valid.

37. A method for a service provider to transmit decryption information in a secure manner, comprising:

receiving a request for a service from a requestor via postal mail;

authenticating the requestor;

transmitting first decryption information to the requestor via postal mail for use in decrypting the service;

transmitting the service, encrypted with encryption information corresponding to the first decryption information, over a unidirectional channel;

generating second decryption information for use in decrypting the service at a later time;

transmitting the second decryption information over the unidirectional channel; and

transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel.

38. The method of claim 37 wherein transmitting first decryption information to the requestor via postal mail includes transmitting a SIM card containing the first decryption information.

39. A method for a service provider to transmit decryption information in a secure manner, comprising:

receiving a request for a service from a requestor;

authenticating the requestor;

installing first decryption information on a device of the requestor for use in decrypting the service;

transmitting the service, encrypted with encryption information corresponding to the first decryption information, over a unidirectional channel;

generating second decryption information for use in decrypting the service at a later time;

transmitting the second decryption information over the unidirectional channel for reception by the requestor; and

transmitting the service, encrypted with encryption information corresponding to the second decryption information, over the unidirectional channel.